Journal of Information & Knowledge Management
Vol. 15, No. 1 (2016) 1650007 (30 pages)

DOI: 10.1142/S0219649216500076

World Scientific
www.worldscientific.com

A Study of Cyber Security Awareness in Educational Environment in the Middle East

Samaher Al-Janabi
Department of Information Networks
Faculty of Information Technology
University of Babylon, Babylon 00964, Iraq
samaher@itnet.uobabylon.edu.iq

Ibrahim Al-Shourbaji
Computer Network Department
Computer Science and Information System College
Jazan University, Jazan 82822-6649, Saudi Arabia
i_shurbaji@yahoo.com

Published 29 January 2016

Abstract. Information security awareness can play an important role in facing cyber-attacks by intruders. The main goal of this paper is to analyse the information security awareness among academic staff, researchers, undergraduate students and employee within educational environments in the Middle East in an attempt to understand the level of awareness of information security, the associated risks and overall impact on the institutions. The results reveal that the participants do not have the requisite knowledge and understanding of the importance of information security principles and their practical application in their day-to-day work. This situation can however be corrected through comprehensive awareness and training programs as well as adopting all the necessary safety measures at all levels of the institution to ensure that the students, academic staff and employees are trustworthy, technology savvy and keep their data safe. Without such training programs and awareness, there will be negative consequences on IT systems and their application usage, as well as on users' personal security now and in the future. From the weaknesses identified in this survey, some essential recommendations are put forward to remedy the situation.

Keywords: Cyber security; information security; safety measures; security awareness; security training policy; digital forensics; classification and regression tree (CART).

1. Introduction

Technological advancements in computing environments and computer applications have led to the development of networks, unregulated social networking, thousands of active users and applications at any given time. Since many of these users and applications are insecure, there exist cybercriminals, masquerades, hackers and anti-social persons seeking to exploit system vulnerabilities (Sabaratnam and Kirby, 2012), particularly in the educational environments (EEs).

The availability of such technology with advanced computing environments, networks and applications is vital for today's online and offline educational processes, and interactions. Students and teachers can get access to unlimited amounts of information to expand not only their learning and knowledge horizons, but also to add to their dynamic educational experiences (Dunn, 2012). Unfortunately, these technologies are proving increasingly difficult to protect from malicious activities. In light of this, the adverse impacts of these incidents including unauthorized access to private and institutional data, identity misuse, intellectual property theft and financial fraud constitute potential threats to critical infrastructure, public safety and national security (Mota and Conradie, 2012).

Apart from providing the necessary protective and security mechanisms, a good awareness program must undergo proper designing to provide compulsory awareness and active training and education programs for users and employees as well. The program should be instrumental in developing and spreading security awareness between them, employing proper physical access controls, obeying the security policies and rules as laid down by the institution/organisation to achieve the best security (McDaniel, 2013).

It is widely thought that there is a direct relation between information security awareness and preventive action, which improves the security performance (Knapp *et al.*, 2006). This suggests that employee security awareness and assessment should be the starting point in developing or enhancing any security strategies.

The employee's intention to comply with information security awareness is significantly influenced by their attitude, normative beliefs and self-worth to comply with overall personal and organisational efficacy (Bulgurcu *et al.*, 2010). Kruger *et al.* found that a significant relationship exists between the knowledge of information security concepts and behaviours that reinforce self-worth and overall credibility (Kruger *et al.*, 2010).

1.1. *Background*

Educational institutions depend on computer networks and technologies to provide their students with university news, activities, emails, courses, academic year calendar, academic staff, student's marks and other personal information stored on their computer systems. Therefore, these systems need to be protected against a number of threats which include malware, spyware, cross site scripting (XSS), viruses, worms, Trojan horse, phishing, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS), (Wilshusen, 2012). It could be used by an adversary not only to affect the organisation's assets by stealing their sensitive information, but to also affect the organisation's financial side. Therefore, every organisation using information systems must take information security seriously.

The last decade has virtually perceived a dramatic increase in the number of cyber-security bugs and cybercrime incidents as well. According to a report in 2014 by Lewis of the Center for Strategic and International Studies (CSIS), Heartbleed is

the recent serious cyber-security vulnerability in open SSL where a number of websites use computer code library called open SSL software. Further, this software is used to encrypt the believed secure websites connections, which are responsible for sending/receiving sensitive information such as, credit card details, online backs transactions, online purchasing, etc. Most importantly, the users using those websites believe they are secured since the software is open source and freely available for anyone to use. This encourages hackers to take advantage to achieve his/her desired goals by accessing the source code to break the encryption or hack the software. In light of this, some organisations such as Gmail encourage their users to change the passwords and even use different passwords while they are accessing different secure websites as a precautionary step to be safe from Heartbleed risk (Hamlen, 2014).

Besides this, the Middle East local media occasionally reports attempts to hack into the banks' electronic systems from website attacks or shutdown. For example, the Bahraini Telco Company and the National bank of Kuwait were both targeted by phishing attacks (Sutton, 2008). On the other hand, the UAE Ministry of Education was infected by a computer virus, UAE Today (2010) and in 2012 Saudi Aramco, the computer network was infected by a computer virus called *Shamoon* and it took almost two weeks to repair the damage (Bronk and Tikk-Ringas, 2013). Thus, information security awareness, education, and training objectives are important and mandatory across all disciplines depending on the institution's information security policy for protecting and minimising cyber-attack risks (Breier and Hudec, 2013).

1.2. *Related work*

Information security awareness is particularly important for sensitive academic information which must at all-time be protected from cyber-attacks that he/she may later use the data for personal advantage. This section briefly presents some of related research in cyber security, as well as information security awareness and training, within the educational sector.

Richardson (2011) of Computer Security Institute (CSI) found that malware infection continues to be the most commonly experienced attack on ICT systems. On the other hand, malware can prove to be an attacking tool for stealing private, business, financial information and other personal information, for example, stealing people's credit card details or to send an email spam, for monitoring user's web browsing behaviour, (Jang-Jaccard and Nepal, 2014). More recently, in 2013, the Kaspersky Lab quoted that about 91% of the organisation surveys reported that their IT Infrastructure had been the target of at least one external attack in the past 12 months. They also reported that malware, spam, phishing, network intrusion and the theft of mobile devices increased significantly compared to 2012 for these five threats (Kaspersky Lab. Global, 2013).

Beside this, Wilshusen (2012) highlights the serious outcomes and effects of cyber incidents on businesses. These incidents include data theft, malicious software

infections and sensitive personal data such as, credit and debit card information, which must be protected against unauthorized use. In addition, it is necessary to identify the source of the threats, types of cyber exploits and the common cyber security technologies that can serve to prevent such threat or to reduce vulnerability of cyber-attacks. The technologies include antivirus software, firewalls, intrusion Detection and prevention systems, computer forensic tools, digital signature and certification as well as Biometrics. This can play a vital role in improving the level of security.

Katz (2005) found that universities have been under cyber-attacks for two main reasons (i) open access to users and information they provide for the public at large and (ii) the vast amount of computing power worth harnessing. He emphasized that a balance must exist between the nature of higher education that provides access to the public for sharing of information and ensuring that information assets stay out of risk. While, Rezgui and Marks (2008) revealed that factors such as, beliefs, cultural values and social conditions affect university staffs' behaviour in relation to how they undertake their work resulting in security and privacy implications. Thus, safety and security measures should be addressed carefully and be essential parts of the academic institutions strategy design.

Kim (2014) conducted a survey of business students in New England to investigate the student's attitude for information security awareness in order to develop an effective Information Security Awareness Training (ISAT). The findings showed that the students understand the need for ISAT and its importance to enhance their awareness level. While, Aloul (2012) showed the need for security awareness in different academic sectors in the Middle East by presenting results of several security awareness studies conducted among students and professionals in the academic sector despite offering little insight on how best to conduct training to reduce security risks. Therefore, information security awareness, education and training are vitally important and should be part of an organisation's overall security management and risk assessment plans for every class of administrators and users to minimize the risk that could be caused by cyber-attacks.

Academic institutions are also vulnerable to cyber-attacks; such examples include heist of patent awards for students and professors, theft of private information for students and faculty staff, (Rajewski, 2013). Thus, in addition to a proper awareness programs, training, education and policies, the educational institutions must include all the safety measures such as, security, privacy, trust, identity management, audit and digital forensics to satisfy the legal and social requirements.

In addition, "simulation tools" can play a vital role in enhancing the information awareness and assurance levels for students, academic staff, and professionals, (Pastor *et al.*, 2010). These tools have several characteristics, they are easy to use and understand, allowing students/users to per form real experiments, and enabling them to understand information security concepts in greates deep. Its main goal is to increase and optimize the level of information security awareness, education,

assurance, and training not only for the students, but also for the academic staff and employees as well.

The usage of the internet has increasingly changed the way people live and has work and has become a necessity in our daily life, not only for entertainment, but also to communicate with those close to us. This plays a vital role in increasing the risk of theft, fraud and abuse. On the other hand, there is no country, industry or even individual that is safe from cyber security incidents risks and its consequences. In turn, security awareness is particularly important for sensitive information that must at all-time be protected from cyber-attacks that he/she may use the data for personal advantage and should be one of the most important priorities for any country as well.

Considering the survey will be instrumental in creating change and awareness, the localization of the survey in respect to considering Middle East constitutes a better approach as opposed to referring to foreign surveys on this topic. In addition, a critical aspect of this survey involves assessing the influence of behaviour in the response, awareness and understanding of cyber-attacks. The dimension of behaviour presents a new angle or perspective of appreciating the underlying issues and concepts of cyber-attack on educational and learning institutions. Additionally, the dynamism of cyber-attacks means that institutions must keep abreast of developments in cyber-attack activities and issues pertaining to information security (Godbole, 2008).

A worldwide range of studies have focussed on the effectiveness of information security in academic sectors (Chan and Mubarak, 2012; Willison and Warkentin, 2013; Kim, 2014). The nature of educational institutions is open access to users and information they provide for the public at large. Due to this, it could increase the chance of accessing personal and private data that include students identifiers, research records, and financial information and could be the primary reason for targeting academic institutions by cyber security incidents and attackers. Considering the survey will be instrumental in creating change and awareness, as well as a better approach as opposed to referring to foreign surveys on the same. In addition, a critical aspect of this survey involves assessing the influence of behaviour in the response, awareness and understanding of cyber-attacks aspects. Awareness against cyber security incidents and their consequences should not to be ignored because it is important to all information security aspects and also their outcomes could affect academic institutions sensitive personal information and their financial data as well. This research was motivated to recognise the degree of awareness of the targeted EE by primarily focussing on the conduct of their academic staff, researchers, undergraduate students and employees in order to determine the grade of their discernment, use for security including all aspects of security measures within the academic environment against cyber security incidents. In addition, since security awareness is paramount, there is a need for focussing primarily on the issue.

The security of information systems is becoming a leading priority nowadays ever more, where the number of cyber security incidents rapidly rises and becomes more

and more effective and aggressive than before. For that, each organisation using information systems must take information security seriously as their top priority. The fact is that information security is a discipline that relies on experts, employee awareness in addition to technical controls to make sure that an organisation's information assets are fully protected. However, in this questionnaire-based survey research, we analyse and evaluate the understanding, awareness, use and problems relating to all information security measures and the weaknesses within some of educational institutions located in different countries in the Middle East to ensure that there exists an understanding of issues relating to the awareness and understanding of cyber-attacks targeting education and learning environment. Based on the survey results, we will offer recommendations that would be valuable in providing a comprehensive overview of the factors that influence compliant information security behaviour. In addition, we need to identify areas that need further research in the academic sector to improve the protection and awareness as well against cyber incidents/crime, and to reduce the damage that could be incurred now and in the future. Our research is based on the following two questions:

- *What is the level of awareness among the target groups for cyber security incidents aspects?*
- *What are recommendations and criteria needed to increase the awareness level and qualify trustworthy?*

2. Research Method

The questionnaire was organised to obtain the level of security awareness, and cyber security for the targeted participants groups. The targeted groups include academic staff, researchers, undergraduate students and employees. The choice of these individuals groups, using information systems as part of their day-to-day job demands, had a basis on the expectation that they were more worried about their private information such as student's marks, exams, research records, etc., in the academic sectors.

The questionnaire was conducted in May 2014. It consists of 26 questions and their answers were limited to "Yes" or "No", the estimated time to complete the questionnaire by participants is about 15 minutes and their criteria were designed to extract and determine the awareness level that the targeted groups have in their understanding of cyber security. The questionnaire focussed on the following and was not limited to threats to information system such as phishing, DoS and DDoS attacks, spam, viruses, etc., and for trustworthy incase of security concepts such as strong password, encryption, authentication and digital forensics. Appendix A shows the overall questions that were used in the questionnaire.

The protocol for this questionnaire was developed based on the study conducted by (Chan and Mubarak, 2012). The authors used an online questionnaire in order to examine the level of employee-information security awareness within higher education domain in South Australia.

The strategies used for distributing the questionnaires in this research included face-to-face interviews, follow-up, phone calls and emails, which made it the choice list as the primary means of distributing the questionnaires. The questionnaire was mailed to 985 participants; however, feedback was slower than expected. To accelerate the response rate, further face-to-face and follow-up phone calls served to keep in touch with participants who had not yet responded, within three weeks after sending out the questionnaires. 760 completed responses were obtained after 7 weeks, which were then used for subsequent data analyses, and assessment. Appendix A shows the overall questions used in our study.

3. Proposed System Phases

The proposed system consists of three main phases as shown in Fig. 1. These include *Pre-processing, clustering the targeted groups answers by using Ant Colony Optimization (ACO) Algorithm, analysing the behaviours and generating the recommendations.* The proposed system executes according to the following phases:

3.1. *The pre-processing phase*

The responses generated many questions relating to security aspects distributed among the people who are working in the EE. When the targeted groups answered the questionnaire, their responses were transformed into binary code 0, and 1 respectively, where 0 means "No", and 1 refers "Yes", then stored in a database to be used for a certain purpose. On the other hand, the behaviour of the participants' answers has been drawn in order to create an image on how the targeted groups dealt with the cyber-security aspects. Unfortunately, the results turn out to be ambiguous and so we cannot depend on those results to take any corrective or crucial decisions for their awareness level. Table 1 shows the correlation between the questions.

The main goal of creating person correlation matrix is to compare the responses of the target groups with the optimal answers to those questions in order to get and identify the questions that are uncorrelated and non-essential as well. Furthermore, is 5 out of 26 questions their optimal answers were No and the rest were Yes. The uncorrelated questions were highlighted in yellow, which include Q1, Q4 and Q10, respectively, as shown in Table 1. Because these questions are uncorrelated with another at least 10 questions and their uncorrelated values are negative, they can be ignored, but we will include them because the main idea and goal of this research is to improve the awareness level of security for the targeted groups. In addition, one cannot delete the real answer of any participants to preserve authenticity and accuracy of the study and its results.

3.2. *Second phase: Clustering the phase based on ACO*

The ACO is a heuristic algorithm that is inspired by the food foraging behaviour of ants. Ant colonies would be able to accomplish tasks that would be impossible to be

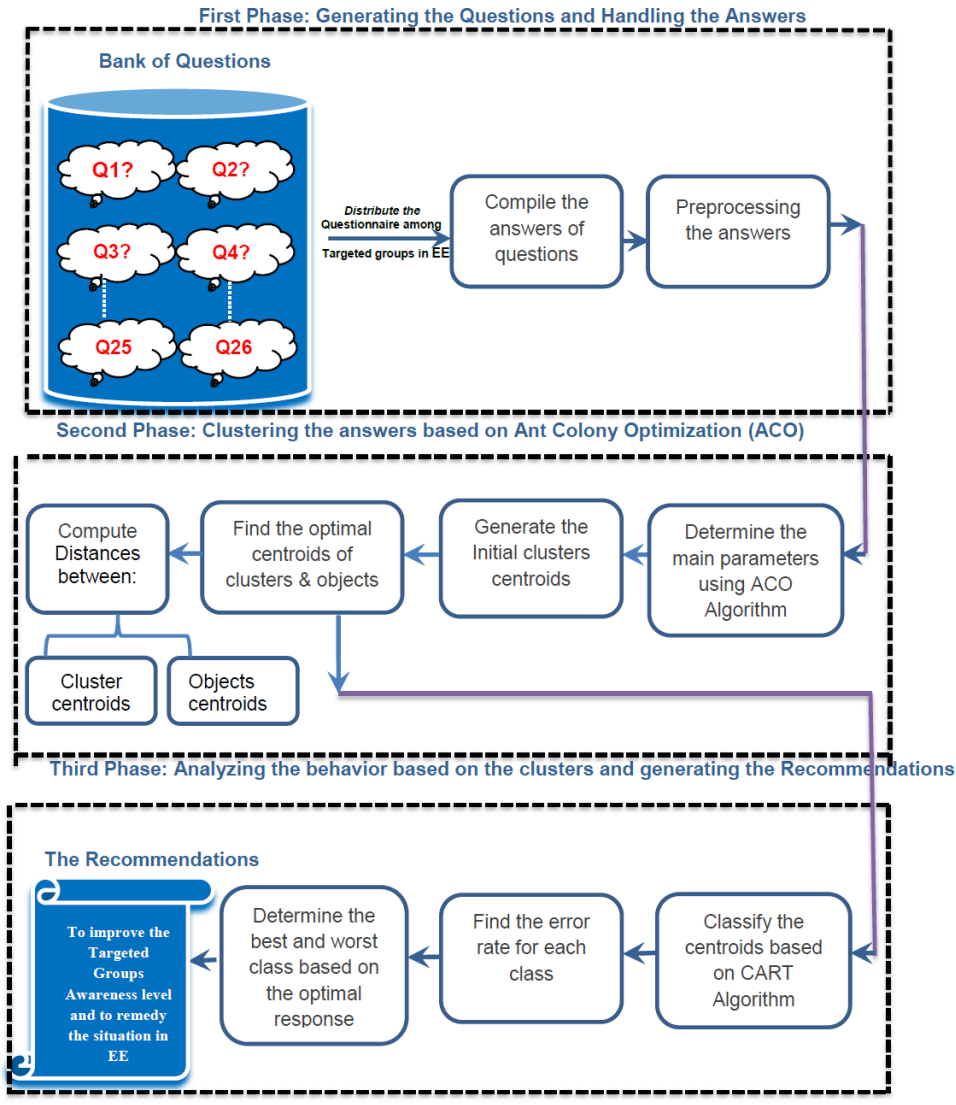

Fig. 1. The phases conducted in our research.

accomplished by a single individual ant. One type of task is seeking the shortest path from their nest to the food source. All foraging ants use the pheromone as a guide regardless of whether the pheromone is deposited by itself or other ants. Pheromones accumulate when multiple ants travel through the same path. The pheromones on the tail evaporate as well. Those ants that reach the food first return before the others. Their return trail's pheromone is now stronger than the other ant trails that have not found food or have longer distances from the food source to nest because the return trail has been travelled twice. This high pheromone volume trail attracts

Table 1. Person correlation among the targeted groups answers in the EE.

Variables	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13
Q 1	**1**	−0.009	**−0.158**	**0.435**	0.005	**−0.293**	**−0.204**	**−0.337**	**−0.190**	**0.618**	**−0.196**	0.004	**−0.156**
Q 2	−0.009	**1**	**0.118**	0.017	**0.193**	**0.342**	**0.184**	**0.255**	**0.123**	0.029	**−0.141**	**0.260**	**0.182**
Q 3	**−0.158**	**0.118**	**1**	**0.260**	**0.334**	**0.371**	−0.025	**0.335**	**0.452**	**0.084**	**0.154**	**0.157**	**0.422**
Q 4	**0.435**	0.017	**0.260**	**1**	**0.366**	**−0.401**	**0.213**	**−0.129**	**0.117**	**0.560**	**−0.271**	**−0.090**	**−0.149**
Q 5	0.005	**0.193**	**0.334**	**0.366**	**1**	**−0.074**	**0.525**	**0.486**	**0.556**	**0.147**	0.061	**0.274**	**0.283**
Q 6	**−0.293**	**0.342**	**0.371**	**−0.401**	**−0.074**	**1**	**−0.179**	**0.426**	**0.192**	**−0.280**	**0.446**	**0.446**	**0.503**
Q 7	**−0.204**	**0.184**	−0.025	**0.213**	**0.525**	**−0.179**	**1**	**0.341**	**0.341**	0.006	−0.020	**0.189**	**0.084**
Q 8	**−0.337**	**0.255**	**0.335**	**−0.129**	**0.486**	**0.426**	**0.341**	**1**	**0.594**	**−0.299**	**0.330**	**0.398**	**0.621**
Q 9	**−0.190**	**0.123**	**0.452**	**0.117**	**0.556**	**0.192**	**0.341**	**0.594**	**1**	**−0.140**	**0.254**	**0.288**	**0.523**
Q 10	**0.618**	0.029	**0.084**	**0.560**	**0.147**	**−0.280**	0.006	**−0.299**	**−0.140**	**1**	**−0.331**	**0.118**	**−0.169**
Q 11	**−0.196**	**−0.141**	**0.154**	**−0.271**	0.061	**0.446**	−0.020	**0.330**	**0.254**	**−0.331**	**1**	**0.212**	**0.205**
Q 12	0.004	**0.260**	**0.157**	**−0.090**	**0.274**	**0.446**	**0.189**	**0.398**	**0.288**	**0.118**	**0.212**	**1**	**0.498**
Q 13	**−0.156**	**0.182**	**0.422**	**−0.149**	**0.283**	**0.503**	**0.084**	**0.621**	**0.523**	**−0.169**	**0.205**	**0.498**	**1**
Q 14	**0.247**	**0.081**	**0.432**	**0.168**	**0.447**	**0.365**	−0.006	**0.236**	**0.379**	**0.288**	**0.225**	**0.421**	**0.468**
Q 15	**−0.187**	**0.103**	**0.427**	**−0.086**	**0.373**	**0.424**	**0.202**	**0.563**	**0.655**	**−0.112**	**0.309**	**0.505**	**0.629**
Q 16	**−0.278**	**0.335**	**0.172**	**−0.294**	**0.102**	**0.668**	0.038	**0.376**	**0.216**	**−0.251**	**0.289**	**0.438**	**0.500**
Q 17	0.020	**0.164**	**0.287**	0.004	**0.297**	**0.461**	**0.106**	**0.440**	**0.437**	−0.009	**0.329**	**0.647**	**0.579**
Q 18	**0.481**	0.059	**0.289**	**0.655**	**0.135**	**−0.163**	−0.060	**−0.252**	−0.061	**0.664**	**−0.328**	**0.088**	−0.056
Q 19	**0.241**	**0.427**	0.031	**0.223**	**0.144**	**0.107**	0.020	−0.027	−0.029	**0.250**	0.031	**0.089**	−0.057
Q 20	−0.070	**0.199**	**0.505**	0.057	**0.279**	**0.473**	−0.028	**0.411**	**0.472**	0.070	**0.164**	**0.567**	**0.638**
Q 21	**0.225**	**0.113**	**0.372**	**0.269**	**0.556**	**0.292**	**0.163**	**0.310**	**0.423**	**0.296**	**0.230**	**0.423**	**0.347**
Q 22	0.007	**0.171**	**0.161**	−0.008	**0.281**	**0.431**	**0.248**	**0.403**	**0.406**	**0.084**	**0.276**	**0.733**	**0.484**
Q 23	**0.122**	**0.105**	**0.221**	**0.134**	**0.458**	**0.129**	**0.284**	**0.355**	**0.411**	**0.099**	**0.156**	**0.266**	**0.233**
Q 24	**0.444**	**0.133**	0.066	**0.219**	**0.264**	0.017	**0.097**	0.052	**0.088**	**0.325**	**−0.200**	**0.231**	**0.185**
Q 25	**−0.292**	**0.277**	**−0.182**	**−0.348**	−0.017	**0.485**	0.052	**0.272**	−0.014	**−0.299**	**0.274**	**0.356**	**0.085**
Q 26	**−0.162**	**0.292**	**0.373**	−0.053	**0.193**	**0.634**	−0.017	**0.495**	**0.272**	−0.031	**0.293**	**0.626**	**0.616**

Variables	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26
Q 1	**0.247**	**−0.187**	**−0.278**	0.020	**0.481**	**0.241**	−0.070	**0.225**	0.007	**0.122**	**0.444**	**−0.292**	**−0.162**
Q 2	**0.081**	**0.103**	**0.335**	**0.164**	0.059	**0.427**	**0.199**	**0.113**	**0.171**	0.105	**0.133**	**0.277**	**0.292**
Q 3	**0.432**	**0.427**	**0.172**	**0.287**	**0.289**	0.031	**0.505**	**0.372**	**0.161**	**0.221**	0.066	**−0.182**	**0.373**

Table 1. (*Continued*)

Variables	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26
Q 4	**0.168**	**−0.086**	**−0.294**	0.004	**0.655**	**0.223**	0.057	**0.269**	−0.008	**0.134**	**0.219**	**−0.348**	−0.053
Q 5	**0.447**	**0.373**	**0.102**	**0.297**	**0.135**	**0.144**	**0.279**	**0.556**	**0.281**	**0.458**	**0.264**	−0.017	**0.193**
Q 6	**0.365**	**0.424**	**0.668**	**0.461**	**−0.163**	**0.107**	**0.473**	**0.292**	**0.431**	**0.129**	0.017	**0.485**	**0.634**
Q 7	−0.006	**0.202**	0.038	**0.106**	−0.060	0.020	−0.028	**0.163**	**0.248**	**0.284**	**0.097**	0.052	−0.017
Q 8	**0.236**	**0.563**	**0.376**	**0.440**	**−0.252**	−0.027	**0.411**	**0.310**	**0.403**	**0.355**	0.052	**0.272**	**0.495**
Q 9	**0.379**	**0.655**	**0.216**	**0.437**	−0.061	−0.029	**0.472**	**0.423**	**0.406**	**0.411**	**0.088**	−0.014	**0.272**
Q 10	**0.288**	**−0.112**	**−0.251**	−0.009	**0.664**	**0.250**	0.070	**0.296**	**0.084**	**0.099**	**0.325**	**−0.299**	−0.031
Q 11	**0.225**	**0.309**	**0.289**	**0.329**	**−0.328**	0.031	**0.164**	**0.230**	**0.276**	**0.156**	**−0.200**	**0.274**	**0.293**
Q 12	**0.421**	**0.505**	**0.438**	**0.647**	**0.088**	**0.089**	**0.567**	**0.423**	**0.733**	**0.266**	**0.231**	**0.356**	**0.626**
Q 13	**0.468**	**0.629**	**0.500**	**0.579**	−0.056	−0.057	**0.638**	**0.347**	**0.484**	**0.233**	**0.185**	**0.085**	**0.616**
Q 14	**1**	**0.517**	**0.427**	**0.633**	**0.278**	**0.221**	**0.541**	**0.818**	**0.478**	**0.428**	**0.396**	**−0.105**	**0.429**
Q 15	**0.517**	**1**	**0.335**	**0.641**	−0.041	−0.068	**0.656**	**0.540**	**0.621**	**0.529**	**0.153**	**0.137**	**0.497**
Q 16	**0.427**	**0.335**	**1**	**0.460**	**−0.159**	**0.151**	**0.493**	**0.259**	**0.399**	**0.093**	**0.122**	**0.448**	**0.585**
Q 17	**0.633**	**0.641**	**0.460**	**1**	**0.102**	**0.078**	**0.616**	**0.531**	**0.689**	**0.293**	**0.273**	**0.141**	**0.666**
Q 18	**0.278**	−0.041	**−0.159**	**0.102**	**1**	0.014	**0.310**	**0.180**	0.036	0.028	**0.260**	**−0.285**	**0.203**
Q 19	**0.221**	−0.068	**0.151**	**0.078**	0.014	**1**	**−0.086**	**0.226**	**0.096**	0.063	−0.016	**0.093**	**0.117**
Q 20	**0.541**	**0.656**	**0.493**	**0.616**	**0.310**	**−0.086**	**1**	**0.390**	**0.472**	**0.265**	**0.272**	**0.097**	**0.670**
Q 21	**0.818**	**0.540**	**0.259**	**0.531**	**0.180**	**0.226**	**0.390**	**1**	**0.621**	**0.588**	**0.381**	0.054	**0.323**
Q 22	**0.478**	**0.621**	**0.399**	**0.689**	0.036	**0.096**	**0.472**	**0.621**	**1**	**0.466**	**0.271**	**0.406**	**0.613**
Q 23	**0.428**	**0.529**	**0.093**	**0.293**	0.028	0.063	**0.265**	**0.588**	**0.466**	**1**	**0.360**	**0.135**	**0.114**
Q 24	**0.396**	**0.153**	**0.122**	**0.273**	**0.260**	−0.016	**0.272**	**0.381**	**0.271**	**0.360**	**1**	−0.023	**0.111**
Q 25	**−0.105**	**0.137**	**0.448**	**0.141**	**−0.285**	**0.093**	**0.097**	0.054	**0.406**	**0.135**	−0.023	**1**	**0.373**
Q 26	**0.429**	**0.497**	**0.585**	**0.666**	**0.203**	**0.117**	**0.670**	**0.323**	**0.613**	**0.114**	**0.111**	**0.373**	**1**

other ants following the trail. The pheromone content on this trail becomes stronger as the trail is increasingly travelled and the other trail's pheromone content becomes weaker because fewer ants travel those trails where the pheromone evaporates. Eventually, the trail with the highest content of pheromone and travelled by most of the foraging ants becomes the shortest tail between food sources to nest.

The main idea of the ACO algorithm is to mimic the ant's foraging behaviour with "simulated ants" walking around the graph searching for the optimal solution where, in the ACO algorithm, each path followed by a "simulated ant" represents a candidate solution to a given problem. The simulated ant "deposits" pheromone on the path and the volume of the pheromone is proportional to the quality of the corresponding candidate solution for the target problem. The searching ants choose the path(s) with the higher volume of pheromone with greater probability than the path(s) with low pheromone volume. Eventually, the searching ants will converge on the path that represent the optimum or near optimum solution for the target problem.

In this research, we will try to use the above idea to cluster the answers of 760 participants. This enables us to ensure that there exists an understanding of issues relating to the awareness and understanding of cyber-attacks targeted and are targeting education environments, and how they deal, use, understand the information security aspects in order to identify the level of awareness they have.

In this phase and based on the ACO, five clusters were built for 760 targeted participants who were asked 26 questions. The main reason to build five clusters is that, there were five questions in which their optimal answers are No (0) and Yes (1) for 21. Class centroids are also built to ensure the number of clusters, with the average of 5. Tables 2 and 3 show the initial value of the clusters.

In order to get the shortest and largest distances between clusters, weights were given to each cluster and the traditional Euclidean distance between the seeds and clusters was calculated. The distances between centroids and object centroids are shown in Tables 4 and 5.

Table 6 shows that in the first step, 138 participants filled out the questionnaire belonging to cluster 1, 106 belong to cluster 2, 148 belong to cluster 3, 168 belong to cluster 4 and 200 belong to cluster 5 respectively. It is important to note that the total of samples is 760, this indicates that all participants' answers are available, and there is no loss to any of them. Figure 2 shows the rate in each cluster.

3.3. *Third phase: Analysing of the behaviours and generating the recommendations*

In this phase, machine learning technique was applied for the Classification and Regression Tree (CART) type in order to classify and separate the behaviours of the participants. CART is one of the DTs techniques that is used to classify data easily in a more understandable form. To classify a data problem, the value of the target

Table 2. Initial values of cluster centroids.

Cluster	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13
1	0.676	0.155	0.777	0.541	0.676	0.365	0.642	0.304	0.459	0.649	0.128	0.655	0.432
2	0.587	0.119	0.846	0.490	0.622	0.455	0.622	0.350	0.510	0.580	0.119	0.657	0.476
3	0.665	0.177	0.772	0.481	0.639	0.449	0.614	0.329	0.487	0.627	0.127	0.696	0.443
4	0.667	0.115	0.833	0.577	0.654	0.353	0.705	0.365	0.494	0.628	0.122	0.641	0.442
5	0.606	0.161	0.806	0.465	0.665	0.523	0.626	0.381	0.458	0.587	0.174	0.748	0.490

Cluster	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26
1	0.709	0.399	0.358	0.486	0.581	0.176	0.622	0.703	0.622	0.703	0.736	0.595	0.615
2	0.748	0.497	0.371	0.622	0.580	0.091	0.615	0.734	0.643	0.734	0.727	0.531	0.629
3	0.772	0.462	0.437	0.608	0.525	0.158	0.658	0.791	0.703	0.741	0.797	0.633	0.633
4	0.737	0.494	0.353	0.583	0.635	0.083	0.622	0.737	0.641	0.724	0.788	0.526	0.603
5	0.800	0.458	0.497	0.639	0.568	0.142	0.645	0.761	0.742	0.723	0.768	0.710	0.735

Table 3. Final values of cluster centroids.

Cluster	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14
1	0.768	0.109	0.971	0.348	0.051	0.906	0.000	0.014	0.087	0.783	0.188	0.797	0.543	0.920
2	0.972	0.585	0.528	0.774	0.962	0.472	0.943	0.368	0.349	0.991	0.038	1.000	0.311	0.906
3	0.081	0.223	1.000	0.000	1.000	1.000	0.858	0.993	0.993	0.000	0.486	1.000	0.993	1.000
4	0.393	0.006	0.446	0.345	0.226	0.018	0.673	0.107	0.167	0.321	0.000	0.280	0.000	0.012
5	1.000	0.000	1.000	1.000	1.000	0.000	0.740	0.285	0.710	1.000	0.000	0.530	0.460	1.000

Cluster	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26	Within-cluster variance
1	0.391	0.587	0.739	0.906	0.116	0.877	0.710	0.739	0.486	0.754	0.645	1.000	3.622
2	0.321	0.689	0.792	0.840	0.575	0.557	1.000	1.000	0.792	0.915	1.000	0.849	3.464
3	1.000	1.000	1.000	0.000	0.007	0.993	1.000	1.000	1.000	0.784	1.000	1.000	0.828
4	0.000	0.030	0.012	0.250	0.000	0.119	0.089	0.262	0.387	0.435	0.673	0.196	3.284
5	0.575	0.000	0.555	0.915	0.105	0.670	1.000	0.550	0.935	0.955	0.000	0.400	2.588

Table 4. Distances between the cluster centroids.

	1	2	3	4	5
1	0	1.915	2.642	2.594	2.232
2	1.915	0	2.530	2.822	1.880
3	2.642	2.530	0	3.581	3.026
4	2.594	2.822	3.581	0	2.666
5	2.232	1.880	3.026	2.666	0

Table 5. Distances between the object centroids.

	1	2	3	4	5
1	0	2.646	3.162	4.243	3.162
2	2.646	0	3.317	4.359	2.646
3	3.162	3.317	0	4.243	3.162
4	4.243	4.359	4.243	0	4.000
5	3.162	2.646	3.162	4.000	0

Table 6. Optimal results of Clustering using ACO.

Cluster	1	2	3	4	5
Objects	138	106	148	168	200
Sum of weights	138	106	148	168	200
Within-cluster variance	3.622	3.464	0.828	3.284	2.588
Minimum distance to centroid	1.361	1.326	0.600	1.355	1.241
Average distance to centroid	1.861	1.823	0.862	1.769	1.584
Maximum distance to centroid	2.694	2.792	2.214	2.649	2.195

variable (Y) is found by using some interesting variable (X). It recursively splits the data from top to bottom to build the tree. Each branch represents a question about the value of one of the X variables to specify which direction the child nodes are to follow, right or left. If there are no more questions to ask in which specific direction to grow, it will terminate into a terminal node. It makes splits dependent only on one variable in each level (Roman, 2004). As a result, more accurate split from a combination of variables may be lost. If the number of variables is high, too many levels will be needed and more computational time will be required.

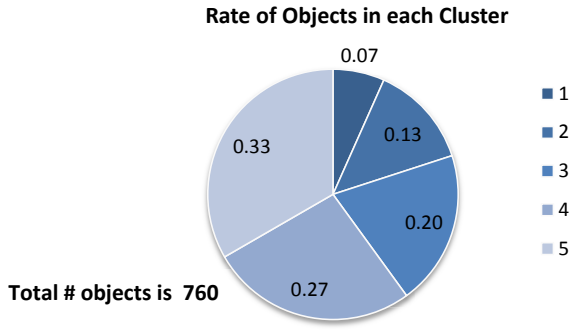

Fig. 2. The optimal distribution of objects among the five clusters.

Pseudo Code of CART

Input: Answers Dataset.

Output: Classification values.

Step 1: Specify Target variable Y.

Step 2: Specify interest variables set X.

Step 3: Starting from the root, for each new node do the following step:

3.1: For each variable $x \in X$.

3.1.1: Sort vector values of x.

3.1.2: Choose best split point s in x according to the following equation:

$$\Delta i(s,t) = i(t) - p_L i(t_L) - p_R i(t_R)$$

3.2: From all split point s choose the one that has lowest impurity.

Step 4: If Split condition is True, then Split node n to new two child nodes nL, nR according to the split point s in variable x from step 3.2.
Else set node n as terminal node.

Step 5: If stopping condition is false, then go to Step 3.
Else go to step 6.

Step 6: Make pruning for Tree until it reaches to optimal size according to re-substitution estimate of the expected squared error according to following equation:

$$R(d) = \frac{1}{N} \sum_{i=1}^{N} (yi - d(xi))2$$

Step 7: After Tree, model is completed, find the values of target variable Y by tracing tree.

Step 8: If terminal node is reached by tracing, then use mean or median to set value of Y.

Step 9: End.

The main equation for computing the results of Step 3.1.2 in the above pseudo code is derived from the following:

$$i(t) = \frac{\sum_{n \in h(t)} w_n f_n (y_n - (t))^2}{\sum_{n \in h(t)} w_n f_n}, \quad p_L = N_w(t_L)/N_w(t), \quad p_R = N_w(t_R)/N_w(t),$$

$$N_w(t) = \sum_{n \in h(t)} w_n f_n, \quad \bar{y}(t) = \frac{\sum_{n \in h(t)} w_n f_n y_n}{N_w(t)}.$$

In this paper, the following initial values were used for each parameter in CART:

The initial value of the complexity parameter is = 0.00000, the minimum size below which the node will not be split = 10, the minimum size for a child node = 1, the node size above which sub-sampling will be used (760 original, 760 copy) = 1520, maximum number of surrogates used for missing values = 5, number of surrogate splits printed = 5, number of competing splits printed = 5, maximum number of trees printed in the tree sequence = 10, maximum number of cases allowed in the learning sample = 1520, maximum number of cases allowed in the test sample = 0, maximum number of non-terminal nodes in the largest tree grown = 759, (Actual number of non-terminal nodes in largest tree grown = 85), maximum number of categorical splits including surrogates = 1, maximum number of linear combination splits in a tree = 0, (actual number cat. + Linear combination splits = 0), maximum depth of largest tree grown = 30, (actual depth of largest tree grown = 13), exponent for centre weighting in split criterion = 1.00000. Table 7 shows the results of CART, it consists of three main parts *top split, left split and right split.* Figure 3 summarizes the main split of CART. Table 8 explains the values of tree optimality

Table 7. CV-tree competitor has three parts.

A. Top Split of CART					
Top split	Competitors				
	Main	1	2	3	4
CV 1	**Q_25**	**Q_10**	**Q_15**	**Q_5**	**Q_9**
	0.5	0.5	0.5	0.5	0.5
	0.00003	0.00003	0.00002	0.00002	0.00002
CV 2	**Q_2**	**Q_15**	**Q_20**	**Q_18**	**Q_8**
	0.5	0.5	0.5	0.5	0.5
	0.00003	0.00003	0.00001	0.00001	0.00001
CV 3	**Q_24**	**Q_5**	**Q_6**	**Q_8**	**Q_13**
	0.5	0.5	0.5	0.5	0.5
	0.00003	0.00003	0.00003	0.00003	0.00002
CV 4	**Q_13**	**Q_20**	**Q_16**	**Q_4**	**Q_15**
	0.5	0.5	0.5	0.5	0.5
	0.00009	0.00005	0.00004	0.00004	0.00003
CV 5	**Q_5**	**Q_25**	**Q_17**	**Q_24**	**Q_16**
	0.5	0.5	0.5	0.5	0.5
	0.00009	0.00003	0.00003	0.00003	0.00002
CV 6	**Q_26**	**Q_5**	**Q_15**	**Q_17**	**Q_2**
	0.5	0.5	0.5	0.5	0.5
	0.00002	0.00002	0.00001	0.00001	0.00001
CV 7	**Q_7**	**Q_18**	**Q_26**	**Q_5**	**Q_13**
	0.5	0.5	0.5	0.5	0.5
	0.00005	0.00004	0.00003	0.00002	0.00002
CV 8	**Q_3**	**Q_22**	**Q_17**	**Q_9**	**Q_4**
	0.5	0.5	0.5	0.5	0.5
	0.00003	0.00002	0.00002	0.00002	0.00002

Table 7. (*Continued*)

A. Top Split of CART					
Top split	Competitors				
	Main	1	2	3	4
CV 9	**Q_17**	**Q_5**	**Q_4**	**Q_14**	**Q_21**
	0.5	0.5	0.5	0.5	0.5
	0.00005	0.00005	0.00005	0.00003	0.00003
CV 10	**Q_12**	**Q_8**	**Q_20**	**Q_3**	**Q_7**
	0.5	0.5	0.5	0.5	0.5
	0.00006	0.00006	0.00005	0.00004	0.00002
FINAL	**Q_25**	**Q_10**	**Q_20**	**Q_1**	**Q_5**
	0.5	0.5	0.5	0.5	0.5
	0	0	0	0	0

B. Left Split of CART					
Left split	Competitors				
	Main	1	2	3	4
CV 1	**Q_6**	**Q_16**	**Q_26**	**Q_22**	**Q_4**
	0.5	0.5	0.5	0.5	0.5
	0.00143	0.00119	0.00087	0.00077	0.00062
CV 2	**Q_16**	**Q_6**	**Q_20**	**Q_19**	**Q_8**
	0.5	0.5	0.5	0.5	0.5
	0.00086	0.00082	0.00065	0.0006	0.00055
CV 3	**Q_1**	**Q_23**	**Q_14**	**Q_10**	**Q_21**
	0.5	0.5	0.5	0.5	0.5
	0.0005	0.00035	0.00034	0.00034	0.00028
CV 4	**Q_15**	**Q_17**	**Q_8**	**Q_9**	**Q_20**
	0.5	0.5	0.5	0.5	0.5
	0.00366	0.00335	0.0033	0.00312	0.00258
CV 5	**Q_9**	**Q_7**	**Q_21**	**Q_8**	**Q_23**
	0.5	0.5	0.5	0.5	0.5
	0.00131	0.0012	0.0011	0.00101	0.00076
CV 6	**Q_17**	**Q_20**	**Q_22**	**Q_12**	**Q_6**
	0.5	0.5	0.5	0.5	0.5
	0.00222	0.00195	0.00186	0.00175	0.00165
CV 7	**Q_5**	**Q_9**	**Q_8**	**Q_23**	**Q_1**
	0.5	0.5	0.5	0.5	0.5
	0.00129	0.00051	0.00048	0.00041	0.00024
CV 8	**Q_20**	**Q_9**	**Q_15**	**Q_13**	**Q_14**
	0.5	0.5	0.5	0.5	0.5
	0.00048	0.00046	0.00038	0.00034	0.00031
CV 9	**Q_22**	**Q_13**	**Q_26**	**Q_15**	**Q_12**
	0.5	0.5	0.5	0.5	0.5
	0.00288	0.00254	0.00233	0.00221	0.00218
CV 10	**Q_22**	**Q_17**	**Q_26**	**Q_13**	**Q_15**
	0.5	0.5	0.5	0.5	0.5

Table 7. (*Continued*)

B. Left Split of CART					
Left split	Competitors				
	Main	1	2	3	4
	0.00202	0.00168	0.00158	0.00144	0.00131
FINAL	**Q_6**	**Q_16**	**Q_26**	**Q_22**	**Q_4**
	0.5	0.5	0.5	0.5	0.5
	0.00143	0.00114	0.00085	0.00085	0.00069

C. Right Split of CART					
Right split	Competitors				
	Main	1	2	3	4
CV 1	**Q_6**	**Q_16**	**Q_26**	**Q_22**	**Q_10**
	0.5	0.5	0.5	0.5	0.5
	0.00257	0.00182	0.00127	0.00116	0.00111
CV 2	**Q_16**	**Q_6**	**Q_19**	**Q_12**	**Q_20**
	0.5	0.5	0.5	0.5	0.5
	0.00014	0.00013	0.00009	0.00008	0.00008
CV 3	**Q_1**	**Q_10**	**Q_14**	**Q_23**	**Q_20**
	0.5	0.5	0.5	0.5	0.5
	0.0017	0.00118	0.00093	0.0009	0.00085
CV 4	**Q_17**	**Q_8**	**Q_15**	**Q_20**	**Q_9**
	0.5	0.5	0.5	0.5	0.5
	0.00273	0.00243	0.00239	0.00239	0.00227
CV 5	**Q_9**	**Q_7**	**Q_8**	**Q_21**	**Q_4**
	0.5	0.5	0.5	0.5	0.5
	0.00264	0.00264	0.00228	0.00208	0.00165
CV 6	**Q_17**	**Q_20**	**Q_22**	**Q_6**	**Q_12**
	0.5	0.5	0.5	0.5	0.5
	0.00382	0.00355	0.00335	0.00326	0.00322
CV 7	**Q_5**	**Q_8**	**Q_9**	**Q_23**	**Q_1**
	0.5	0.5	0.5	0.5	0.5
	0.00251	0.00096	0.00074	0.00061	0.00049
CV 8	**Q_20**	**Q_15**	**Q_9**	**Q_6**	**Q_13**
	0.5	0.5	0.5	0.5	0.5
	0.00193	0.00151	0.00145	0.00115	0.00105
CV 9	**Q_22**	**Q_26**	**Q_13**	**Q_15**	**Q_12**
	0.5	0.5	0.5	0.5	0.5
	0.00419	0.00388	0.00388	0.00382	0.00349
CV 10	**Q_22**	**Q_17**	**Q_26**	**Q_13**	**Q_15**
	0.5	0.5	0.5	0.5	0.5
	0.00456	0.00416	0.00353	0.00322	0.00289
FINAL	**Q_6**	**Q_16**	**Q_26**	**Q_22**	**Q_4**
	0.5	0.5	0.5	0.5	0.5
	0.00215	0.0017	0.00127	0.00127	0.00103

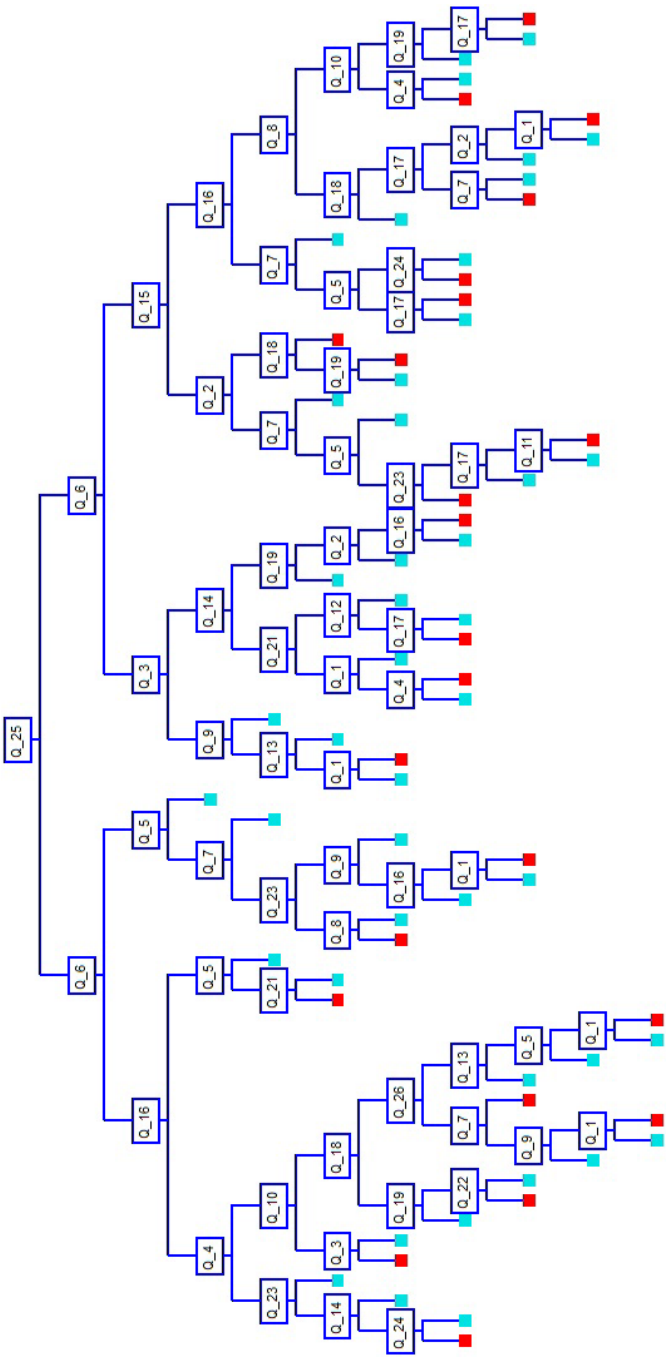

Fig. 3. The main split of CART classifier.

Table 8. Tree optimality criteria.

Terminal		Cross valid rel error	Resub rel error	Test set ROC	Tst set 10% Lift
Tree	Nodes				
1	71	0.1710526	0.0473684	0.9484765*	1.8639227
2	67	0.1710526*	0.0486842	0.9475935	1.8623345
3	58	0.1802632	0.0605263	0.9472992	1.8435581
4	54	0.1842105	0.0684211	0.9427199	1.8214495
5	49	0.2105263	0.081579	0.938608	1.8342078
6	47	0.2092105	0.0881579	0.9384176	1.8342078
7	41	0.2131579	0.1118421	0.9350762	1.8315904
8	35	0.2184211	0.1394737	0.9314751	1.8892191
9	33	0.2539474	0.15	0.91424	1.8778844
10	30	0.2671053	0.1697368	0.9099723	1.8888171
11	28	0.275	0.1842105	0.9064231	1.8938347
12	26	0.2815789	0.2	0.900831	1.8938347*
13	25	0.2960526	0.2092105	0.8878809	1.8490745
14	21	0.2973684	0.2486842	0.8866257	1.8490745
15	20	0.3236842	0.2592105	0.8762292	1.7716135
16	18	0.3618421	0.2881579	0.8621191	1.7300657
17	16	0.3710526	0.3210526	0.8586825	1.7511183
18	15	0.3934211	0.3381579	0.8536184	1.8197063
19	11	0.4657895	0.425	0.8088296	1.6844495
20	10	0.5105263	0.45	0.778705	1.6186752
21	8	0.5276316	0.506579	0.7623269	1.5522961
22	7	0.6171053	0.5394737	0.7085007	1.3812497
23	6	0.7131579	0.6065789	0.6609245	1.3280484
24	5	0.7421053	0.6802632	0.65058	1.3374108
25	1	1	1	0.5	1

Note: * refers to values that duplicated more than once.

criteria. Finally, the analysis of classification model (CART) based on Gains chart appears with all details in Fig. 4.

Table 9 shows the behaviour analysis of the targeted groups within EE. The participant's answer to the questions matching the ideal answer is kept in a white colour, otherwise, another colour is given in the box. Table 10 shows the meaning of each colour.

The proposed system can convert the ambiguity of behaviours of the targeted people in EE to become understandable and perfectly acceptable behaviours by classifying the participants into five classes based on their deal with the security aspects and their responses to the questionnaire. On the other side, the error rate is executed according to the following equation:

$$\text{The Error Rate} = (\#\text{False Answer}/26),$$

where it is equal to the number of wrong answers from each cluster on the total number of questions. In this way, we will be able to decide which cluster out of 5 has the best answers for the participants, with their percentage and the error rate.

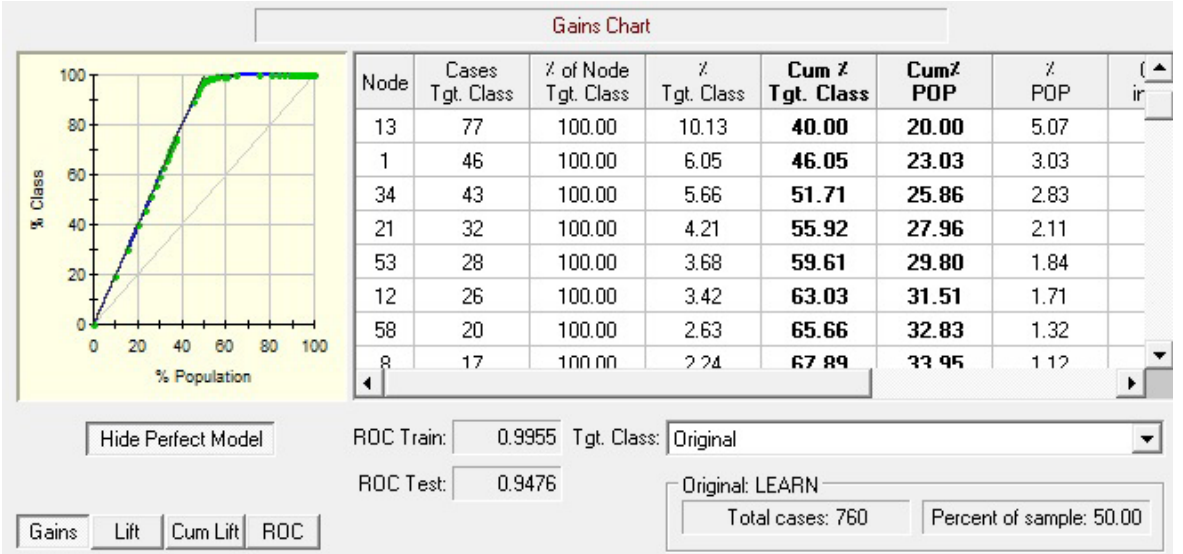

Fig. 4. Test of model based on gains.

Table 9. Analysis of the behaviours of targeted groups in the EE based on their dealing with security aspects.

Questions	Q 1	Q 2	Q 3	Q 4	Q 5	Q 6	Q 7	Q 8	Q 9	Q 10	Q 11	Q 12	Q 13	Q 14	Q 15	Q 16	Q 17	Q 18	Q 19	Q 20	Q 21	Q 22	Q 23	Q 24	Q 25	Q 26
GI																										
LI																										
VGI																										
VLI																										
SI																										

Table 10. The meaning of the colours.

Colour	Description
	Meaning the participants' answers in the class number one were not matched the optimal answers
	Meaning the participants' answers in the class number two were not matched the optimal answers
	Meaning the participants' answers in the class number three were not matched the optimal answers
	Meaning the participants' answers in the class number four were not matched the optimal answers
	Meaning the participants' answers in the class number five were not matched the optimal answers

Table 11. Percentage of the participants' awareness level.

Colour	The Participants' Awareness Level
	The participants have a good information (GI) of security aspects and their rate is 18% out of the 760 who involved in the questionnaire
	The participants have low information (LI) of security aspects and their rate is 14% out of the 760 who involved in the questionnaire
	The participants have very good information (VGI) of security aspects rate of 20% out of the 760 who involved in the questionnaire
	The participants have very low information (VLI) of security aspects rate of 22% out of the 760 who involved in the questionnaire
	The participants have simple information (SI) of security aspects rate of 26% out of the 760 who involved in the questionnaire

Table 12. Analysis of the participants' behaviour based on their responses to the questionnaire.

Class	Objects	Error Rate
GI	138	0.307692308
LI	106	0.423076923
VGI	148	0.153846154
VLI	168	0.846153846
SI	200	0.384615385

Best Answer

Worst Answer

Table 11 shows the participants level with their percentages and Table 12 shows which cluster has the worst/best answers (with their computed number) and the margin of error rate.

This paper vividly gave a crucial pointer about the level of information security awareness within the EE in reference to information security awareness as well. Consequently, EE's need for information security awareness can be in the form of a set of safety measures and recommendations to secure their sensitive data and to ensure that data are kept safe as well as to increase the awareness level.

4. Discussion and Findings

Generally, the proposed system approved that there is a clear lack of knowledge of information security concepts, as well as a low levels of awareness within the EEs. Although the results were still very immature and alarming about information security awareness as defined by Bulgurcu *et al.* (2010). Additionally, the results show a clear lack of knowledge of information security concepts, as well as generally low levels of awareness. However, it provided a generic look at the level of information security awareness in the academic environment; despite the belief that security starts with awareness for everyone (Furnel and Clarke, 2012; Hinson, 2013). Furthermore, if our participants' awareness is increased, it would result in increased network security and protection and avoidance from being victims of hacking. This is also observed by Hinson's work (2013).

Kruger *et al.* (2010) "identified significant relationships between knowledge of the concepts and behaviour". That is, our knowledge of the concept translates to positive behaviour in relation to the concept. However, the present study is in contrast with Kruger's perception. Bulgurcu *et al.* (2010) also recognised such a large variance and suggested that information security with regard to concepts is often built upon life experience.

Cyber security awareness should undergo meticulous designing and formulation by the academic institutions at the enterprise level of top management as the highest authority responsible for all kinds of security affecting their users, students, academic staff and employees. These policies should then be carried through and executed at all levels of management to ensure protection and compliance.

Yeo *et al.* (2007) suggested that the lack of awareness represents a serious problem to any organisation and should be properly assessed as part of the organisation's overall security management and assessment strategy. Furthermore, Hu *et al.* (2012) and Goo *et al.* (2013) both suggested that the policy should come from the top management of the academic enterprise, so it can be administered properly by the IT services to enjoy the support and compliance by the users in terms of their obligations to use the facilities and services. In addition to this, the users must control and manage their behaviours for any security breaches as stated in the guidelines and statutes of the academic institution pertaining to the overall law of the country and other international regulatory bodies because they can be

considered as a root cause for security breaches (Hu *et al.*, 2012). Once the security risks/consequences are assessed, they undergo minimization by improving security awareness through educating/training programs within the academic institution's environment by conducting seminars or workshops to encourage the active use of these security services and facilities, (Chan and Mubarak, 2012; McDaniel, 2013).

Encryption methods and security software are necessary to protect our sensitive data, but the results show that for question 8, 40% did not attempt to use either the encryption method or software. This represents a highly negative percentage compared to the CSI computer crime and security survey (Richardson, 2011). They also found that viruses and unauthorized access to the system have the highest incidents.

In summary, our findings extend information-security research literature by confirming and substantiating the following:

(1) Information security awareness and training should be part of an organisation's overall security management and risk assessment plans for all classes of administrators and users.
(2) Information directives and guidelines should undergo a clear and accurate explanation in the simplest non-jargon language.
(3) There is great importance in the need to mitigate all kinds of security risk by providing information security awareness, and educating/training programs, workshops, seminars as well as posters at regular intervals, and to encourage the active use of security services and facilities within the academic institutions.
(4) The input of third party support in attaining complete information security can make the difference in the fight against cyber-attacks. This analysis, therefore, illustrates that learning institutions can consider outsourcing computing power and security services to their advantage.
(5) A lot of literature on information security is oriented to business information systems and the wider field of information communication technology. Despite the fact that the underlying technology and computing environments remain more or less the same across the board, the perspective of information security in relation to educational institutions provides a new addition to existing literature. In essence, the focus on information security in educational institutions broadens the scope of awareness towards possibilities of cyber-attacks targeting educational and learning institutions.

5. Recommendations

It is also highly recommended that information security measures in learning institutions should entail regular information backups to ensure that at every given moment, the institutions have copies of all critical data and information that can serve as restoration points in the case of data and information loss, corruption and compromise. This also ensures there is continuity of operations (contingency plan) in the case of data loss or corruption. In essence, the institutions should consider

continuity of operation in the event of an information security breach. A recommended approach to this end involves enlisting the services of a hot site where an external company or third party provides disaster recovery service through continuation of computerized and networked systems to facilitate the storage and dissemination of information systems in wake of information security breaches (Estall, 2012). A good example of this kind of service is the use of cloud computing services from credible service providers who provide quality services based on superior technology and advanced security components.

According to (Patel *et al.*, 2015), the safety measures are vital to adopt the legal and social requirements. In a broader perspective, academic institutions have to include all safety measures within their environments. The reason for this is to ensure their students, academic staff and the employees' data are trustworthy within the academic environment. These measures include:

- Concept of negotiation-contract approach in order to increase the level of trust.
- Intrusion Detection and Prevention Systems (IDPS).
- Trust.
- Privacy and Identity Management.
- Audit and Digital forensics.

Data security denotes the bulwark and protection of information, including systems and hardware that use, store and transmit that information. Security and protection include many aspects at the application level such as, authentication, authorization, confidentiality, integrity and availability. This aspect is important and plays a vital role in protecting the data stored on academic institutions systems. There are several methods providing protection such as, sandboxing, authentication, authorization, proof-carrying code and e-payment check, (Ou and Ou, 2010) which can be used for protecting academic institutions assets.

Another important security and privacy measure is to create awareness among students about cyber security and privacy. This is because some of them do not have an understanding of this type of incidents and the devastating consequences that it can cause, and therefore, are not be in a position to make balanced judgments concerning the extent to which it may have a negative impact on their own perceived standards of privacy (Patel *et al.*, 2015). Cyber security awareness should start from academic staff to students by teaching about cyber incidents consequences and risks within workshops, classrooms. Teachers should also educate what is new in this field and in this way will ensure a clearer picture of awareness level at the individual and institutional levels.

It is also highly recommended that information security measures in academic institutions should have specialized labs for digital forensics to teach the students about computer crimes, mobile forensics, investigation techniques, analysing illegal events in order to collect digital evidences, etc. Even more important is digital forensics as an activity of investigation to trace and analyse illegal and fraudulent

events to produce evidence for the purpose of law enforcement. Intrusion Detection and Prevention Systems (IDPS) can assist digital forensics since it can prove to be an invaluable tool, where its goal is to perform early detection, trace of malicious activity, and possibly prevent more serious damage to the protected systems. Thus, an IDPS is a very useful tool for collecting and interpreting digital evidences that may be used in a court of law purposes. It also can draw the big picture of what is going on in the systems and can test the effectiveness of the control environment within academic institutions by identifying policies and attributes that breach security, privacy and trust rules.

In this struggle, to secure information such as the data of students, academic staff, employees, research records, and financial data on which it is stored in the systems, Information Security Management System (ISMS) can play a vital role in improving and managing information security aspects, where its goal is to identify approaches, strategic decisions and methodologies to ensure that the data is kept away from risks and threats as well as kept safe (Fahey, 2013). ISMS can also be a very useful tool to bridge the gap between management and technical people were both parties have to understand that security is not something that could be ignored and it is one of the most important factors to achieve the desired goals in any organisation. It is vitally recommended that academic institutions implementing of an ISMS in their environment should ensure that the data of students, academic staff, and employees are kept safe. Furthermore, an ISMS such as, ISO/IEC 27001: 2013 (ISO 27001:2013, 2013) which represents one of the most widely used standards can help academic institutions to ensure that the security of their private data are secured at all levels as well as improve the effectiveness of their information security.

Finally, academic institutions must take serious steps towards a better level of consciousness to ensure acceptance of such awareness framework or program. It will also need both actual and non-actual regulatory and standard bodies, governments, higher education institutions and industry to address the safety measure issues to synthesize legislations, directives, and guidelines for the academic institutions as part of their comprehensive deployment strategy.

6. Conclusion

Our aim from this questionnaire-based survey research was to analyse information security and evaluate the understanding, awareness, use and problems relating to all information security safety measures and their weaknesses within some of the educational institutions located in different countries in the Middle East. The questionnaires were specifically outlined to analyse all information security aspects including the taxonomy of the level of information security within the academic institution. The results show a degree of success with respect to achievement of desired goals. Our questionnaire focussed on user awareness as well as safety measures as part of the information security concepts. Furthermore, our questionnaires serve to investigate the knowledge of the awareness level of common information

security concepts and the behaviours as well as reactions of the targeted groups regarding the security concepts within the EE. However, the overall results indicate that the targeted groups lack awareness of all cyber security incidents and their consequences. Based on the weaknesses identified in this survey, recommendations come into the foreground as suggested solutions in overcoming them. This would also require the awareness framework to meet the need for the other substantive safety measures such as trust, identity management, audit, digital forensics, and information-system management security to ensure compliance with the law and ethical behaviour by academic institutions to safeguard their personal and information data now and in the future.

Appendix A

This appendix contains the overall questions were used in the Questionnaire.

A Study of Cyber Security Awareness in Academic Institutions

Questions	Answer	
	Yes	No
When you receive an email from an unfamiliar sender, do you open it?		
When you receive an email requiring your credential informations such as, name, date of birth, age, your credit card number? Do you send it?		
Do you receive by emails sweepstakes, win a lottery, select to receive a prize in cash, offered to partner in a huge money transfer transaction, or had been promised to receive gift cards?		
Do you shop/purchase items advertised on social network or on your private email?		
Do you know some characteristics to a good password, and always employ one when accessing secure websites?		
Do you know, what is the meaning of concept phishing?		
Do you use the same passwords for both social networks such as, Facebook, Twitter, iTunes, and your personal email accounts?		
Do you think that it is important to read the user agreements for free program/software before clicking, "I accept"?		
Do you know "what is the difference between using http and https"?		
Do you use debit or credit card at an outdoor payment machine?		
Do you know what social engineering is?		
Do you use the computer of office for work only in your specific field?		
Do you know, what are DoS and DDoS attacks mean and its effects as well?		
Did you download free Software/Programs from the internet?		
Did you try to use encryption method or encryption software to protect your sensitive information?		
Do you regularly check the update of antivirus software that it used on your computer/ laptop?		
Did you use backup software to backup your important data?		
Do you think, a totally rely on technology and the available software security in preventing such an attack?		

Appendix A. (*Continued*)

A Study of Cyber Security Awareness in Academic Institutions

Questions	Answer	
	Yes	No
In case receiving a phone call from an individual who says he is student's father and asking for his marks, is it correct to give out that information?		
Do you think is it important to provide authentication for online courses to ensure proper monitoring for exams and assignments?		
Do you think, privacy policies and procedures with regard the use of personal identification are one of the responsibilities of students, staff or top management such as dean, vice president, IT support staff or researchers?		
Do you think that security should be addressed within academic institutions environment and should cover all aspects such as, confidentiality, integrity, availability, authentication, authorization?		
Do you think Information security awareness is responsible from students, academic staff and top management?		
Is there a need for digital forensics department in academic institutions to trace any illegal events to produce evidence for the purpose of law?		
In your opinion, is it important that the academic institutions to have an information security officer?		
Do you desire to learn more on security?		

References

Aloul, FA (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, 3(3).

Breier, J and L Hudec (2013). On identifying proper security mechanisms. In *Information and Communication Technology*. pp. 285–294, Berlin: Springer, doi: 10.1007/978-3-642-36818-9_29.

Bronk, C and E Tikk-Ringas (2013). The cyber-attack on saudi aramco. *Survival*, 55(2), 81–96, doi: 10.1080/00396338.2013.784468.

Bulgurcu, B, H Cavusoglu and I Benbasat (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *IS Quarterly*, 34(3), 523–548.

Chan, H and S Mubarak (2012). Significance of information security awareness in the higher education sector. *International Journal of Computer Applications*(0975–8887), 60(10), doi: 10.5120/9729-4202.

Dunn, J (2012). The importance of internet access in schools. Available at http://www.edudemic.com/2012/12/the-importance-of-internet-access-in-schools/. Accessed on 15 September 2013.

Estall, H (2012). *Business Continuity Management Systems: Implementation and Certification to* ISO 22301, United Kingdom: BCS, The Chartered Institute.

Fahey, R (2013). Human factors in information security management systems. Available at http://www.springer.com/computer/security+and+cryptology/journal/10207?detailsPage=pltci_1060167. Accessed on 13 September 2013.

Furnel, S and N Clarke (2012). Power to the people? The evolving recognition of human aspects of security. *Computer and Security*, 31(8) 983–988.

Godbole, N (2008). *Information Systems Security: Security Management, Metrics, Frameworks And Best Practices (With CD)*. Wiley, p. 1020.

Goo, J, MS Yim and DJ Kim (2013). A path way to successful management of individual intention to security compliance: A role of organizational security climate. In *Proceedings of International Conference on System Sciences (HICSS)*, 46th Hawaii, pp. 2959–2968, doi: 10.1109/HICSS.2013.51.

Hamlen, K (2014). Cybersecurity researchers roll out a new heartbleed solution. Availablility at http://www.utdallas.edu/news/2014/4/14-29531_Cybersecurity-Researchers-Roll-Out-A-Heartbleed-So_story-wide.html. Accessed on 18 April 2014.

Hinson, G (2013). The true value of information security awareness. A living white paper, conceived in 2003 and most recently updated in 2013. Availability at http://www. noticebored.com/html/why_awareness_.html. Accessed on 13 September 2013.

Hu, Q, T Dinev, P Hart and D Cooke (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture*. *Decision Sciences*, 43(4), 615–660, doi: 10.1111/j.1540-5915.2012.00361.

ISO 27001:2013 (2013). Information security management certification documents, Available at http://www.isoconsultant.us/iso-27001-certifications-standards-manual-documentation-audit-checklist.htm. Accessed on 15 September 2013.

Jang-Jaccard, J and S Nepal (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973–993.

Kaspersky Lab. Global (2013). IT Security Risks. Available at http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf. Accessed on 3 September 2013.

Katz, FH (2005). The effect of a university information security survey on instructing methods in information security. In *Proceedings of the 2nd Annual Conference on Information Security Curriculum Development*, Kennesaw, GA, USA, pp. 43–48.

Kim, EB (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, 22(1), 115–126, doi: 10.1108/IMCS-01-2013-0005.

Knapp, KJ, TE Marshall, KR Rainer, NF Ford (2006). Information security: Management's effect on culture and policy. *Information Management & Computer Security*, 14(1), 24–36.

Kruger, H, L Drevin and T Steyn (2010). A vocabulary test to assess information security Awareness. *Information Management & Computer Security*, 18(5), 316–327.

McDaniel, EA (2013). Securing the information and communications technology global supply chain from exploitation: Developing a strategy for education, training, and awareness. *Issues in Informing Science and Information Technology*, 10, 313–324.

Mota, M and P Conradie (2012). Evaluating the current state of network security threats in academic institutions. *Advanced Research in Scientific Area*, 1. Available at http://arsa-conf.com/archive/?vid=1&aid=2&kid=60101-60.

Ou, CM and CR Ou (2010). SETNR/A: an agent-based secure payment protocol for mobile commerce. *International Journal of Intelligent Information and Database Systems*, 4(3), 212–226. doi: 10.1504/IJIIDS.2010.034080.

Pastor, V, G Díaz and M Castro (2010). State-of-the-art simulation systems for information security education, training and awareness. In *Proceedings of Education Engineering (EDUCON)*, pp. 1907–1916, IEEE, doi: 10.1109/EDUCON.2010.5492435.

Patel, A, S Al-Janabi, I AlShourbaji and J Pedersen (2015). A novel methodology towards a trusted environment in mashup web applications. *Computers & Security*, 49, 107–122.

Rajewski, J (2013). Cyber security awareness: Why higher education institutions need to address digital threats. Available at http://www.huffingtonpost.com/jonathan-rajewski/cyber-security-awareness-_b_4025200.html. Accessed on 14 April 2014.

Rezgui, Y and A Marks (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7–8), 241–253.

Richardson, R (2011). Computer crime and security survey, computer security institute. Available at http://www.ncxgroup.com/wp-content/uploads/2012/02/CSIsurvey2010.pdf. Accessed on 15 August 2013.

Roman, T (2004). Classification and regression trees (CART) theory and applications, Master thesis, Humboldt University, Berlin.

Sabaratnam, M and P Kirby (2012). Open access: hefce, ref2020 and the threat to academic freedom. Available at http://thedisorderofthings.files.wordpress.com/2012/12/open-Access-hefce-and-ref2020-position-paper3.pdf. Accessed on 15 July 2013.

Sutton, M (2008). Batelco internet subscribers targeted by phishing attack. Arabian Business. Available at http://www.arabianbusiness.com/520459-batelco-internetsubscribers-targeted-by-phishing-attack. Accessed on 3 September 2013.

UAE Today (2010). Internet virus infects Ministry of Education. Available at http://www.emaratalyoum.Com/local section/accidents/2010-04-12-1.106891. Accessed on 3 September 2012.

Willison, R and M Warkentin (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly Journal*, 37(1), 1–20.

Wilshusen, GC (2012). Information security cyber threats facilitate ability to commit economic espionage. US Governments Accountability Office. Available at http://www.gao.gov/assets/600/592008.pdf. Accessed on 3 September 2013.

Yeo, AC, MM Rahim and L Miri (2007). Understanding factors affecting success of information security risk assessment: The case of an Australian higher educational institution. In *PACIS Proceedings*, 74pp.